

**STANDARD FORMAT SPECIFICATION FOR AUTOMATICALLY
CONFIGURING IP SECURITY TUNNELS**

BACKGROUND OF THE INVENTION

5

1. Technical Field:

The present invention relates in general to a method and system for securing networks. Still more particularly, the present invention relates to an improved system and method for providing a standard format to use to configure IP security tunnels where the standard format may be used by any one of multiple, different operating systems and multiple, different machine types.

15

2. Description of Related Art:

In today's modern environment, many businesses and organizations deal with global markets and have global logistic concerns. Many organizations have facilities disbursed across the country or even around the world. Despite their global presence, these organizations need a way to maintain fast, secure and reliable communications with individuals and other offices throughout the world.

Until recently, fast, secure and reliable communication has meant the use of leased lines to maintain a Wide Area Network (WAN). Leased lines, ranging from ISDN (Integrated Services Digital Network, 144 Kbps) to OC3 (Optical Carrier-3, 155 Mbps) fiber, provided a company with a way to expand their private network beyond their immediate geographic area. A WAN had obvious advantages over a public network like the Internet when it came to reliability, performance and

Docket No. AUS920010449US1

security. But maintaining a WAN, particularly when using leased lines, can become quite expensive and often rises in cost as the distance between the offices increases. In addition, using WANs is not a scaleable solution as
5 the number of interconnections rises exponentially as new locations are added.

In essence, a Virtual Private Network, or "VPN," is a private network that uses a public network (usually the Internet) to connect remote sites or users together. To
10 make communication between computers private, VPNs use security methods, such as encryption, to maintain privacy. Instead of using a dedicated, real-world connection such as a leased line, a VPN uses "virtual" connections routed through the Internet from the
15 company's private network to the remote site or employee.

A well-designed VPN can greatly benefit a company. For example, it can: extend geographic connectivity, improve security, reduce operational costs versus traditional WAN, reduce transit time and transportation
20 costs for remote users, improve productivity, simplify network topology, provide global networking opportunities, provide telecommuter support, provide broadband networking compatibility, and provide faster ROI (Return On Investment) than traditional WAN. A
25 well-designed VPN, therefore, should incorporate features for security, reliability, scalability, network management, and policy management.

In a VPN, each remote member of the network is able to communicate in a secure and reliable manner using the
30 Internet as the medium to connect to a private local area network, or "LAN." A VPN can grow to accommodate more users and different locations much easier than a leased

Docket No. AUS920010449US1

line. In fact, scalability is a major advantage that
VPNs have over typical leased lines. Unlike leased
lines, where the cost increases in proportion to the
distances involved, the geographic locations of each
5 office matter little in the creation of a VPN.

A well-designed VPN uses several methods for keeping
connections and data secure. Firewalls provide a strong
barrier between private networks and the Internet.
Firewalls can restrict the number of open ports, what
10 type of packets are passed through, and which protocols
are allowed through. Encryption is used to encode all
the data that one computer is sending to another into a
form that only the other computer will be able to decode.
Two modes of authentication are used on VPNs: pre-shared
15 keys and digital signatures.

Pre-shared key encryption means that each partner in
a VPN has a secret "key" that it can use to authenticate
the remote identifier of a VPN. Pre-shared key
encryption requires that you know which computers will
20 talk to each other, and that you install the same key on
each one.

Digital signature authentication, on the other hand,
uses a combination of a private key and a public key.
The private key is known only to your computer while the
25 public key is given by your computer to any computer that
wants to communicate securely with it. To decode an
encrypted message, the receiving computer must use the
public key provided by the originating computer. Public
keys are bound to an identity, such as a business or a
30 user, by using "digital certificates" that are typically
issued by a trusted third party.

Docket No. AUS920010449US1

The key is based on a hash value. This is a value that is computed from a base input number using a hashing algorithm. The important thing about a hash value is that it is nearly impossible to derive the original input
5 number without knowing the data used to create the hash value. Public keys generally use complex algorithms and very large hash values for encrypting.

On a typical VPN, the authentication of the initial connection is accomplished using public key algorithm.
10 Once the connection is established and authenticated, keying material is sent from one computer to the other and the connection switches to symmetric encryption, such as DES or Triple DES. Symmetric encryption is used during data transfer because the amount of time decoding
15 data is reduced.

The Internet Protocol Security Protocol (IPsec) provides enhanced security features such as strong encryption algorithms and comprehensive authentication. IPsec has two encryption modes: tunnel and transport.
20 Tunnel mode tunnels the original packet and builds a new IP header, while transport mode inserts the IPsec payload between the IP header and the data. Systems that are IPsec compliant can take advantage of this protocol. Also, all devices negotiate security parameters, but they
25 must have compatible security policies set up. IPsec works well on both Remote-Access and Site-to-Site VPNs. IPsec must be supported at both tunnel interfaces to work.

The IPsec protocol can be used in conjunction with
30 the Internet Key Exchange security protocol (IKE). This protocol provides additional authentication and encryption features to the IPsec standard.

Docket No. AUS920010449US1

Many VPNs rely on tunneling to create a private network that reaches across the Internet. Essentially, tunneling is the process of placing an entire packet within another packet and sending it over a network. The
5 protocol of the outer packet is understood by the network and both points, called tunnel interfaces, where the packet enters and exits the VPN. Tunneling uses three different protocols: (1) carrier protocol: the protocol used by the network that the information is traveling
10 over; (2) encapsulating protocol: the protocol that is wrapped around the original data; and (3) passenger protocol: the original data (IPX, NetBeui, IP) being carried.

Tunneling has important implications for VPNs. For
15 example, a packet that uses a protocol not supported on the Internet (such as NetBeui) can be placed inside an IP packet and sent it safely over the Internet. Or a packet that uses a private (non-routable) IP address can be placed inside a packet that uses a globally unique IP
20 address in order to extend a private network over the Internet. Tunneling is also necessary for gateways because the IP header needs to have the gateway IP address in it.

An analogy of tunneling is having a computer
25 delivered to you by a courier service. The vendor packs the computer (passenger protocol) into a box (encapsulating protocol) which is then put on a courier truck (carrier protocol) at the vendor's warehouse (entry tunnel interface). The truck (carrier protocol) travels
30 over the highways (Internet) to your home (exit tunnel interface) and delivers the computer. You open the box (encapsulating protocol) and remove the computer

Docket No. AUS920010449US1

(passenger protocol).

The Internet Protocol Security Protocol (IPsec) is a set of open standards. These standards are implemented in a variety of different ways by each different operating system that supports these standards. Therefore, a computer system that is initiating a communication may implement the Internet Protocol Security Protocol in one way while a computer system that is a responder computer system may implement IPsec in a different way.

In known systems when a system administration needs to configure a tunnel between two computer systems that implement the IPsec protocol in different ways, the system administration must configure the tunnel manually by directly inputting the various necessary parameters. This process of manually configuring the security tunnels can become very time consuming, especially in systems requiring many different tunnels.

Therefore, a need exists for a method, system, and product for automatically configuring an IP security tunnel utilizing a standardized security policy specification format in computer systems using any one of different operating systems.

SUMMARY OF THE INVENTION

A data processing system, method, and product are disclosed for automatically configuring IP security tunnels. A security policy specification format is established that is capable of being utilized by any one of multiple different operating systems and any one of multiple different machine types. The format specifies a plurality of different elements that may be used to define a configuration of an IP security tunnel.

In order to define an IP security tunnel configuration, a system administrator first generates an XML file utilizing the elements defined by the standard format. This XML file defines the configuration of a particular IP security tunnel. The configuration of multiple IP security tunnels may be compared by comparing their respective XML files.

The XML file may be used by any type of machine type and any type of operating system. When the XML file is processed, it will automatically configure an IP security tunnel as defined by the elements included in the file.

The format includes elements to define the various parameters defined by the IPsec protocol and the Internet Key Exchange (IKE) protocol. The format includes elements to define separate IKE and IPsec protections. Elements are also included to describe remote and local end points, groups, and pre-shared keys.

When the format is used, tunnels can be configured to a large number of endpoints easily, quickly, and programmatically.

Docket No. AUS920010449US1

The above as well as additional objectives, features, and advantages of the present invention will become apparent in the following detailed written description.

100 101 102 103 104 105 106 107 108 109 110 111 112 113 114 115 116 117 118 119 120 121 122 123 124 125 126 127 128 129 130 131 132 133 134 135 136 137 138 139 140 141 142 143 144 145 146 147 148 149 150 151 152 153 154 155 156 157 158 159 160 161 162 163 164 165 166 167 168 169 170 171 172 173 174 175 176 177 178 179 180 181 182 183 184 185 186 187 188 189 190 191 192 193 194 195 196 197 198 199 200 201 202 203 204 205 206 207 208 209 210 211 212 213 214 215 216 217 218 219 220 221 222 223 224 225 226 227 228 229 230 231 232 233 234 235 236 237 238 239 240 241 242 243 244 245 246 247 248 249 250 251 252 253 254 255 256 257 258 259 260 261 262 263 264 265 266 267 268 269 270 271 272 273 274 275 276 277 278 279 280 281 282 283 284 285 286 287 288 289 290 291 292 293 294 295 296 297 298 299 300 301 302 303 304 305 306 307 308 309 310 311 312 313 314 315 316 317 318 319 320 321 322 323 324 325 326 327 328 329 330 331 332 333 334 335 336 337 338 339 340 341 342 343 344 345 346 347 348 349 350 351 352 353 354 355 356 357 358 359 360 361 362 363 364 365 366 367 368 369 370 371 372 373 374 375 376 377 378 379 380 381 382 383 384 385 386 387 388 389 390 391 392 393 394 395 396 397 398 399 400 401 402 403 404 405 406 407 408 409 410 411 412 413 414 415 416 417 418 419 420 421 422 423 424 425 426 427 428 429 430 431 432 433 434 435 436 437 438 439 440 441 442 443 444 445 446 447 448 449 450 451 452 453 454 455 456 457 458 459 460 461 462 463 464 465 466 467 468 469 470 471 472 473 474 475 476 477 478 479 480 481 482 483 484 485 486 487 488 489 490 491 492 493 494 495 496 497 498 499 500 501 502 503 504 505 506 507 508 509 510 511 512 513 514 515 516 517 518 519 520 521 522 523 524 525 526 527 528 529 530 531 532 533 534 535 536 537 538 539 540 541 542 543 544 545 546 547 548 549 550 551 552 553 554 555 556 557 558 559 560 561 562 563 564 565 566 567 568 569 570 571 572 573 574 575 576 577 578 579 580 581 582 583 584 585 586 587 588 589 590 591 592 593 594 595 596 597 598 599 600 601 602 603 604 605 606 607 608 609 610 611 612 613 614 615 616 617 618 619 620 621 622 623 624 625 626 627 628 629 630 631 632 633 634 635 636 637 638 639 640 641 642 643 644 645 646 647 648 649 650 651 652 653 654 655 656 657 658 659 660 661 662 663 664 665 666 667 668 669 670 671 672 673 674 675 676 677 678 679 680 681 682 683 684 685 686 687 688 689 690 691 692 693 694 695 696 697 698 699 700 701 702 703 704 705 706 707 708 709 710 711 712 713 714 715 716 717 718 719 720 721 722 723 724 725 726 727 728 729 730 731 732 733 734 735 736 737 738 739 740 741 742 743 744 745 746 747 748 749 750 751 752 753 754 755 756 757 758 759 760 761 762 763 764 765 766 767 768 769 770 771 772 773 774 775 776 777 778 779 780 781 782 783 784 785 786 787 788 789 790 791 792 793 794 795 796 797 798 799 800 801 802 803 804 805 806 807 808 809 810 811 812 813 814 815 816 817 818 819 820 821 822 823 824 825 826 827 828 829 830 831 832 833 834 835 836 837 838 839 840 841 842 843 844 845 846 847 848 849 850 851 852 853 854 855 856 857 858 859 860 861 862 863 864 865 866 867 868 869 870 871 872 873 874 875 876 877 878 879 880 881 882 883 884 885 886 887 888 889 890 891 892 893 894 895 896 897 898 899 900 901 902 903 904 905 906 907 908 909 910 911 912 913 914 915 916 917 918 919 920 921 922 923 924 925 926 927 928 929 930 931 932 933 934 935 936 937 938 939 940 941 942 943 944 945 946 947 948 949 950 951 952 953 954 955 956 957 958 959 960 961 962 963 964 965 966 967 968 969 970 971 972 973 974 975 976 977 978 979 980 981 982 983 984 985 986 987 988 989 990 991 992 993 994 995 996 997 998 999 1000 1001 1002 1003 1004 1005 1006 1007 1008 1009 1010 1011 1012 1013 1014 1015 1016 1017 1018 1019 1020 1021 1022 1023 1024 1025 1026 1027 1028 1029 1030 1031 1032 1033 1034 1035 1036 1037 1038 1039 1040 1041 1042 1043 1044 1045 1046 1047 1048 1049 1050 1051 1052 1053 1054 1055 1056 1057 1058 1059 1060 1061 1062 1063 1064 1065 1066 1067 1068 1069 1070 1071 1072 1073 1074 1075 1076 1077 1078 1079 1080 1081 1082 1083 1084 1085 1086 1087 1088 1089 1090 1091 1092 1093 1094 1095 1096 1097 1098 1099 1100 1101 1102 1103 1104 1105 1106 1107 1108 1109 1110 1111 1112 1113 1114 1115 1116 1117 1118 1119 1120 1121 1122 1123 1124 1125 1126 1127 1128 1129 1130 1131 1132 1133 1134 1135 1136 1137 1138 1139 1140 1141 1142 1143 1144 1145 1146 1147 1148 1149 1150 1151 1152 1153 1154 1155 1156 1157 1158 1159 1160 1161 1162 1163 1164 1165 1166 1167 1168 1169 1170 1171 1172 1173 1174 1175 1176 1177 1178 1179 1180 1181 1182 1183 1184 1185 1186 1187 1188 1189 1190 1191 1192 1193 1194 1195 1196 1197 1198 1199 1200 1201 1202 1203 1204 1205 1206 1207 1208 1209 1210 1211 1212 1213 1214 1215 1216 1217 1218 1219 1220 1221 1222 1223 1224 1225 1226 1227 1228 1229 1230 1231 1232 1233 1234 1235 1236 1237 1238 1239 1240 1241 1242 1243 1244 1245 1246 1247 1248 1249 1250 1251 1252 1253 1254 1255 1256 1257 1258 1259 1260 1261 1262 1263 1264 1265 1266 1267 1268 1269 1270 1271 1272 1273 1274 1275 1276 1277 1278 1279 1280 1281 1282 1283 1284 1285 1286 1287 1288 1289 1290 1291 1292 1293 1294 1295 1296 1297 1298 1299 1300 1301 1302 1303 1304 1305 1306 1307 1308 1309 1310 1311 1312 1313 1314 1315 1316 1317 1318 1319 1320 1321 1322 1323 1324 1325 1326 1327 1328 1329 1330 1331 1332 1333 1334 1335 1336 1337 1338 1339 1340 1341 1342 1343 1344 1345 1346 1347 1348 1349 1350 1351 1352 1353 1354 1355 1356 1357 1358 1359 1360 1361 1362 1363 1364 1365 1366 1367 1368 1369 1370 1371 1372 1373 1374 1375 1376 1377 1378 1379 1380 1381 1382 1383 1384 1385 1386 1387 1388 1389 1390 1391 1392 1393 1394 1395 1396 1397 1398 1399 1400 1401 1402 1403 1404 1405 1406 1407 1408 1409 1410 1411 1412 1413 1414 1415 1416 1417 1418 1419 1420 1421 1422 1423 1424 1425 1426 1427 1428 1429 1430 1431 1432 1433 1434 1435 1436 1437 1438 1439 1440 1441 1442 1443 1444 1445 1446 1447 1448 1449 1450 1451 1452 1453 1454 1455 1456 1457 1458 1459 1460 1461 1462 1463 1464 1465 1466 1467 1468 1469 1470 1471 1472 1473 1474 1475 1476 1477 1478 1479 1480 1481 1482 1483 1484 1485 1486 1487 1488 1489 1490 1491 1492 1493 1494 1495 1496 1497 1498 1499 1500 1501 1502 1503 1504 1505 1506 1507 1508 1509 1510 1511 1512 1513 1514 1515 1516 1517 1518 1519 1520 1521 1522 1523 1524 1525 1526 1527 1528 1529 1530 1531 1532 1533 1534 1535 1536 1537 1538 1539 1540 1541 1542 1543 1544 1545 1546 1547 1548 1549 1550 1551 1552 1553 1554 1555 1556 1557 1558 1559 1560 1561 1562 1563 1564 1565 1566 1567 1568 1569 1570 1571 1572 1573 1574 1575 1576 1577 1578 1579 1580 1581 1582 1583 1584 1585 1586 1587 1588 1589 1590 1591 1592 1593 1594 1595 1596 1597 1598 1599 1600 1601 1602 1603 1604 1605 1606 1607 1608 1609 1610 1611 1612 1613 1614 1615 1616 1617 1618 1619 1620 1621 1622 1623 1624 1625 1626 1627 1628 1629 1630 1631 1632 1633 1634 1635 1636 1637 1638 1639 1640 1641 1642 1643 1644 1645 1646 1647 1648 1649 1650 1651 1652 1653 1654 1655 1656 1657 1658 1659 1660 1661 1662 1663 1664 1665 1666 1667 1668 1669 1670 1671 1672 1673 1674 1675 1676 1677 1678 1679 1680 1681 1682 1683 1684 1685 1686 1687 1688 1689 1690 1691 1692 1693 1694 1695 1696 1697 1698 1699 1700 1701 1702 1703 1704 1705 1706 1707 1708 1709 1710 1711 1712 1713 1714 1715 1716 1717 1718 1719 1720 1721 1722 1723 1724 1725 1726 1727 1728 1729 1730 1731 1732 1733 1734 1735 1736 1737 1738 1739 1740 1741 1742 1743 1744 1745 1746 1747 1748 1749 1750 1751 1752 1753 1754 1755 1756 1757 1758 1759 1760 1761 1762 1763 1764 1765 1766 1767 1768 1769 1770 1771 1772 1773 1774 1775 1776 1777 1778 1779 1780 1781 1782 1783 1784 1785 1786 1787 1788 1789 1790 1791 1792 1793 1794 1795 1796 1797 1798 1799 1800 1801 1802 1803 1804 1805 1806 1807 1808 1809 1810 1811 1812 1813 1814 1815 1816 1817 1818 1819 1820 1821 1822 1823 1824 1825 1826 1827 1828 1829 1830 1831 1832 1833 1834 1835 1836 1837 1838 1839 1840 1841 1842 1843 1844 1845 1846 1847 1848 1849 1850 1851 1852 1853 1854 1855 1856 1857 1858 1859 1860 1861 1862 1863 1864 1865 1866 1867 1868 1869 1870 1871 1872 1873 1874 1875 1876 1877 1878 1879 1880 1881 1882 1883 1884 1885 1886 1887 1888 1889 1890 1891 1892 1893 1894 1895 1896 1897 1898 1899 1900 1901 1902 1903 1904 1905 1906 1907 1908 1909 1910 1911 1912 1913 1914 1915 1916 1917 1918 1919 1920 1921 1922 1923 1924 1925 1926 1927 1928 1929 1930 1931 1932 1933 1934 1935 1936 1937 1938 1939 1940 1941 1942 1943 1944 1945 1946 1947 1948 1949 1950 1951 1952 1953 1954 1955 1956 1957 1958 1959 1960 1961 1962 1963 1964 1965 1966 1967 1968 1969 1970 1971 1972 1973 1974 1975 1976 1977 1978 1979 1980 1981 1982 1983 1984 1985 1986 1987 1988 1989 1990 1991 1992 1993 1994 1995 1996 1997 1998 1999 2000 2001 2002 2003 2004 2005 2006 2007 2008 2009 2010 2011 2012 2013 2014 2015 2016 2017 2018 2019 2020 2021 2022 2023 2024 2025 2026 2027 2028 2029 2030 2031 2032 2033 2034 2035 2036 2037 2038 2039 2040 2041 2042 2043 2044 2045 2046 2047 2048 2049 2050 2051 2052 2053 2054 2055 2056 2057 2058 2059 2060 2061 2062 2063 2064 2065 2066 2067 2068 2069 2070 2071 2072 2073 2074 2075 2076 2077 2078 2079 2080 2081 2082 2083 2084 2085 2086 2087 2088 2089 2090 2091 2092 2093 2094 2095 2096 2097 2098 2099 2100 2101 2102 2103 2104 2105 2106 2107 2108 2109 2110 2111 2112 2113 2114 2115 2116 2117 2118 2119 2120 2121 2122 2123 2124 2125 2126 2127 2128 2129 2130 2131 2132 2133 2134 2135 2136 2137 2138 2139 2140 2141 2142 2143 2144 2145 2146 2147 2148 2149 2150 2151 2152 2153 2154 2155 2156 2157 2158 2159 2160 2161 2162 2163 2164 2165 2166 2167 2168 2169 2170 2171 2172 2173 2174 2175 2176 2177 2178 2179 2180 2181 2182 2183 2184 2185 2186 2187 2188 2189 2190 2191 2192 2193 2194 2195 2196 2197 2198 2199 2200 2201 2202 2203 2204 2205 2206 2207 2208 2209 2210 2211 2212 2213 2214 2215 2216 2217 2218 2219 2220 2221 2222 2223 2224 2225 2226 2227 2228 2229 2230 2231 2232 2233 2234 2235 2236 2237 2238 2239 2240 2241 2242 2243 2244 2245 2246 2247 2248 2249 2250 2251 2252 2253 2254 2255 2256 2257 2258 2259 2260 2261 2262 2263 2264 2265 2266 2267 2268 2269 2270 2271 2272 2273 2274 2275 2276 2277 2278 2279 2280 2281 2282 2283 2284 2285 2286 2287 2288 2289 2290 2291 2292 2293 2294 2295 2296 2297 2298 2299 2300 2301 2302 2303 2304 2305 2306 2307 2308 2309 2310 2311 2312 2313 2314 2315 2316 2317 2318 2319 2320 2321 2322 2323 2324 2325 2326 2327 2328 2329 2330 2331 2332 2333 2334 2335 2336 2337 2338 2339 2340 2341 2342 2343 2344 2345 2346 2347 2348 2349 2350 2351 2352 2353 2354 2355 2356 2357 2358 2359 2360 2361 2362 2363 2364 2365 2366 2367 2368 2369 2370 2371 2372 2373 2374 2375 2376 2377 2378 2379 2380 2381 2382 2383 2384 2385 2386 2387 2388 2389 2390 2391 2392 2393 2394 2395 2396 2397 2398 2399 2400 2401 2402 2403 2404 2405 2406 2407 2408 2409 2410 2411 2412 2413 2414 2415 2416 2417 2418 2419 2420 2421 2422 2423 2424 2425 2426 2427 2428 2429 2430 2431 2432 2433 2434 2435 2436 2437 2438 2439 2440 2441 2442 2443 2444 2445 2446 2447 2448 2449 2450 2451 2452 2453 2454 2455 2456 2457 2458 2459 2460 2461 2462 2463 2464 2465 2466 2467 2468 2469 2470 2471 2472 2473 2474 2475 2476 2477 2478 2479 2480 2481 2482 2483 2484 2485 2486 2487 2488 2489 2490 2491 2492 2493 2494 2495 2496 2497 2498 2499 2500 2501 2502 2503 2504 2505 2506 2507 2508 2509 2510 2511 2512 2513 2514 2515 2516 2517 2518 2519 2520 2521 2522 2523 2524 2525 2526 2527 2528 2529 2530 2531 2532 2533 2534 2535 2536 2537 2538 2539 2540 2541 2542 2543 2544 2545 2546 2547 2548 2549 2550 2551 2552 2553 2554 2555 2556 2557 2558 2559 2560 2561 2562 2563 2564 2565 2566 2567 2568 2569 2570 2571 2572 2573 2574 2575 2576 2577 2578 2579 2580 2581 2582 2583 2584 2585 2586 2587 2588 2589 2590 2591 2592 2593 2594 2595 2596 2597 2598 2599 2600 2601 2602 2603 2604 2605 2606 2607 2608 2609 2610 2611 2612 2613 2614 2615 2616 2617 2618 2619 2620 2621 2622 2623 2624 2625 2626 2627 2628 2629 2630 2631 2632 2633 2634 2635 2636 2637 2638 2639 2640 2641 2642 2643 2644 2645 2646 2647 2648 2649 2650 2651 2652 2653 2654 2655 2656 2657 2658 2659 2660 2661 2662 2663 2664 2665 2666 2667 2668 2669 2670 2671 2672 2673 2674 2675 2676 2677 2678 2679 2680 2681 2682 2683 2684 2685 2686 2687 2688 2689 2690 2691 2692 2693 2694 2695 2696 2697 2698 2699 2700 2701 2702 2703 2704 2705 2706 2707 2708 2709 2710 2711 2712 2713 2714 2715 2716 2717 2718 2719 2720 2721 2722 2723 2724

BRIEF DESCRIPTION OF THE DRAWINGS

The novel features believed characteristic of the invention are set forth in the appended claims. The invention itself, however, as well as a preferred mode of use, further objectives and advantages thereof, will best be understood by reference to the following detailed description of an illustrative embodiment when read in conjunction with the accompanying drawings, wherein:

Figure 1 is a system diagram showing a single computer using multiple tunnels to communicate with various VPNs;

Figure 2 is a diagram showing tunnels being created between a computer and other computers using VPN configuration data and certificate data;

Figure 3 is a database diagram showing tables used in configuring tunnels between the computer and other computer systems;

Figure 4 illustrates a high level flow chart which depicts the creation of a phase 1 tunnel using VPN configuration data in accordance with the present invention;

Figure 5 depicts a high level flow chart which illustrates the details involved in creating a secure phase 1 tunnel using the VPN configuration data in accordance with the present invention;

Figure 6 illustrates a high level flow chart which depicts the steps performed in using policies to communicate through phase 1 and phase 2 processing in accordance with the present invention;

Figure 7 depicts a high level flow chart which illustrates establishing a standard format to use by any

Docket No. AUS920010449US1

operating system and any machine type to automatically
configure IP security tunnels in accordance with the
present invention; and

Figure 8 illustrates a high level flow chart which
5 depicts automatically configuring an IP security tunnel
using a standard format in accordance with the present
invention.

FIG. 8 is a high level flow chart illustrating the process of automatically configuring an IP security tunnel using a standard format in accordance with the present invention. The process begins at step 800, where a user selects a machine type and operating system. This selection leads to step 810, where the system automatically configures the IP security tunnel based on the selected machine type and operating system. The process then proceeds to step 820, where the system automatically configures the IP security tunnel using a standard format. Finally, the process ends at step 830.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT

A preferred embodiment of the present invention and its advantages are better understood by referring to the
5 figures, like numerals being used for like and corresponding parts of the accompanying figures.

The invention is preferably realized using a well-known computing platform, such as an IBM RS/6000 server running the IBM AIX operating system. However, it
10 may be realized in other popular computer system platforms, such as an IBM personal computer running the Microsoft Windows operating system or a Sun Microsystems workstation running operating systems such as UNIX or LINUX, without departing from the spirit and scope of the
15 invention.

Figure 1 shows a system diagram of a single computer using multiple tunnels to communicate with various virtual private networks (VPNs). Computer system **100** is shown using computer network **110**, such as the Internet,
20 to communicate with computers using three VPNs - VPN "A" (**120**), VPN "B" (**140**), and VPN "C" (**160**). Three tunnels are shown connecting computer system **100** to first computer system **130**, second computer system **150**, and third computer system **170**. First computer system **130** is
25 shown as a member of VPN "A" (**120**), second computer system **150** is shown as a member of VPN "B" (**140**), and third computer system **170** is shown as a member of VPN "C" (**160**). Each of the VPNs may use a different authentication means to secure the data traveling between
30 the computer systems. For example, computers within VPN "A" **120** may use a pre-shared key (i.e., a common key

Docket No. AUS920010449US1

shared amongst the computers used to derive encryption keys). VPN "B" **140**, on the other hand, may use public key encryption to encrypt the data. Finally, VPN "C" **160** may use digital signatures with digital certificates
5 verified by a trusted third party, also called a "certification authority," or "CA".

Further each of these computers may be implemented using different hardware, i.e. different machine types. Each computer system may also be utilizing a different
10 operating system.

Figure 2 shows a diagram of tunnels being created between a computer and other computers using VPN configuration data and certificate data. Computer system **200** establishes various tunnels used to securely transmit
15 data to and from other computer systems. Computer systems that computer system **200** wishes to securely communicate with over a VPN are identified in VPN configuration database **210**. VPN data **220** contains information for connecting with a particular computer
20 system. Using VPN configuration database **210**, any number of VPNs can be established between computer system **200** and other computer systems. Some VPNs use certificate data **280** supplied by a trusted third party computer system **270**. The use of a trusted third party aids in
25 authenticating users and ensuring that an impostor does not take the place of another computer system.

In the example shown, computer system **200** establishes tunnel A **235** securely connecting first computer system **230** with computer system **200**. Likewise,
30 tunnel B **245** securely connects second computer system **240** with computer system **200**, tunnel C **255** securely connects

Docket No. AUS920010449US1

third computer system **250** with computer system **200**, and tunnel D **265** securely connects fourth computer system **260** with computer system **200**. Each of these computer systems, **230**, **240**, **250**, and **260**, have identification
5 information and authentication information stored in VPN configuration database **210**.

Figure 3 shows a database diagram of tables used in configuring tunnels between the computer and other computer systems. VPN configuration database **300** is
10 shown with four tables. Endpoints table **310** includes a list of configured tunnels between the computer system and other computer systems. One end of each endpoint identifies the computer system, while the other end of the endpoint identifies a remote computer. Each of the
15 computers included in endpoints table **310** is identified with an identifier, such as an address. In addition, endpoints table **310** includes IP addresses for the remote computer systems. An IP address is an identifier for a computer or device on a TCP/IP network. Networks using
20 the TCP/IP protocol route messages based on the IP address of the destination. The format of an IP address is a 32-bit numeric address written as four numbers separated by periods. Each number can be zero to 255. For example, 1.160.10.240 could be an IP address. Within
25 an isolated network, IP addresses can be assigned at random so long as each one is unique. However, connecting a private network to the Internet requires using registered IP addresses (called Internet addresses) to avoid duplicates. The four numbers in an IP address
30 are used in different ways to identify a particular network and a host on that network. Finally, endpoints table **310** includes a flag indicating whether a

Docket No. AUS920010449US1

Certificate Revocation List (CRL) is used to check whether a given certificate has been revoked. Other valid ID types include FQDN, user@FQDN, distinguished names, and key IDs.

5 Endpoints table **310** has relationships with three other tables in VPN configuration database **300**. Each local-remote computer pair included in endpoints table **310** may have a pre-shared key stored in pre-shared keys table **330** or a public key stored in digital certificate table **340**. In some situations, a local-remote computer pair may have both a pre-shared key and a public key. Finally, a policy from policy table **320** exists for one or more set of endpoints determining the access method and preference order for connecting the local computer to a
10 given remote computer.

15 Policy table **320** is used to employ a connection policy used by a given VPN. Typically, one policy exists for each VPN that the local machine uses. Policy table **320** includes the available secure access methods, such as
20 pre-shared key and digital certificates, that are available in using the VPN. In addition, policy table **320** includes a preference order for establishing secure connections when multiple access methods are available. For example, a VPN may prefer using digital certificates
25 to establish secure connections. However, if the computer system is unable to make a secure connection using a digital certificate, a pre-shared key method may also be available as a second course of action.

 Pre-shared keys table **330** includes a list of common,
30 or shared, keys for each tunnel pair that uses a pre-shared key security method. Computers using a pre-shared key have the same key to derive encryption and

Docket No. AUS920010449US1

decryption keys. The pre-shared key is often provided to the computer system or the user in a way to reduce the chance that the key is misappropriated. For example, a pre-shared key may be mailed from a company to a client.

- 5 The client then uses the pre-shared key to establish secure communications with the company computer system. Different pre-shared keys are used for each combination of computer systems. In this manner, if one pre-shared key is compromised only data at the two systems using
10 that key are in jeopardy.

Digital certificate table **340** includes a list of certificates (Public Keys) for each tunnel pair that uses digital certificates to secure communications. In addition, digital certificate table **340** may include
15 signing digital certificate keys used for Certificate Revocation List servers to determine whether a given certificate has been revoked. Public key encryption uses a private key to encrypt information destined for a given computer system. The receiving computer system deciphers
20 the information by using the sender's public key. The local computer system's private key is also included in digital certificate table **340**.

- Figure 4** shows a flowchart of the creation of a tunnel using VPN configuration data. Processing
25 commences at **400** whereupon a remote computer identifier is retrieved (input **405**) corresponding to a remote computer to be connected in a VPN with the current computer system. The remote computer ID is typically received from a user command or IKE message. The remote
30 computer ID is retrieved for both the initiator and the responder. The local-remote endpoints pair corresponding to the remote computer system identifier and the local

Docket No. AUS920010449US1

computer identifier is selected from the endpoints table (step **410**). The ID Rules List links the local-remote endpoints pair to a security policy name that is used in selecting the security policy (see step **440**). A

5 determination is made as to whether the endpoints pair was found (decision **415**). If the pair was not found, decision **415** branches to "no" branch **420** whereupon an error is reported that the user needs to configure a tunnel with the remote computer system before the tunnel
10 can be used (step **425**) and processing terminates (end **430**). Additionally, step **425** could invoke a configuration screen allowing the user to configure the tunnel with the remote computer by supplying the needed access information.

15 If the pair was found in the endpoints table, decision **415** branches to "yes" branch **435** whereupon a policy corresponding to the local-remote pair is selected from the policy table (step **440**). The policy includes a proposal list with separate initiator and responder
20 proposals. Proposals have general characteristics, like lifetimes and transform names. Transforms include specific encryption algorithms, hash algorithms, and authentication methods being proposed. A determination is made as to whether a corresponding policy was found
25 (decision **445**). If a corresponding policy was not found, decision **445** branches to "no" branch **450** whereupon a default policy is used (step **455**). For example, a default policy could be used to use a digital certificate (if available), before attempting to use any available
30 pre-shared keys. If the policy is found, decision **445** branches to "yes" branch **460**.

The initiator proposes one or more authentication methods to the responder in the order of initiator's preference (predefined process **465**, see **Figure 6** for further details). The initiator receives the responder's selection of an authentication method (step **470**). A determination is made as to whether an error occurred in receiving the responder's selection (decision **475**). If an error occurred, decision **475** branches to "yes" branch **480** whereupon processing terminates at **485**. On the other hand, if an error did not occur, decision **475** branches to "no" branch **488** whereupon a secure phase 1 tunnel is created between the initiator and the responder for setting up the phase 2 negotiations to select security choices for data traffic (predefined process **490**, see **Figure 5** for further details). Predefined process **490** includes validating IDs, certificates, or pre-shared keys as well as checking the "liveliness" of the connection that the other computer matches the retrieved endpoint computer description during the entire conversation. After predefined process **490**, create phase 1 tunnel processing terminates at **495**.

Figure 5 shows a flowchart of the details involved in creating a secure tunnel using the VPN configuration data. Processing commences at **500** whereupon the local computer connects to the remote computer using the selected authentication method (step **505**). A determination is made as to whether the authentication method uses a digital certificate (decision **510**). If the authentication method uses a digital certificate, decision **510** branches to "yes" branch **545** whereupon certificate processing commences.

Docket No. AUS920010449US1

On the other hand, if the access method does not use a digital certificate, decision **510** branches to "no" branch **515** whereupon a pre-shared key corresponding to the remote computer system is selected from the pre-shared key table (step **520**). A determination is made as to whether the pre-shared key is found (decision **525**). If the pre-shared key is not found, decision **525** branches to "no" branch **526** whereupon an error is returned at **590**.

If the pre-shared key is found, decision **525** branches to "yes" branch **528** whereupon the local machine attempts to connect to the remote machine using the selected pre-shared key (step **530**). A determination is made as to whether the local machine successfully connected to the remote machine (decision **535**). If the local machine did not successfully connect to the remote machine, decision **535** branches to "no" branch **536** whereupon an error is returned at **590**. On the other hand, if the local machine successfully connects to the remote machine, decision **535** branches to "yes" branch **538** whereupon processing returns to the calling routine (return **595**, see **Figure 4**).

Figure 6 is a flowchart showing steps performed in using policies to communicate through phase 1 and phase 2 processing.

In Phase 1, Initiator **600** commences by proposing (step **610**) specifications, authentication methods, and encryption algorithms to responder **605**. Responder, in turn, receives the proposal (step **615**) and selects an authentication method, specifications, and an encryption algorithm from the proposal and returns the selection to the initiator (step **620**). Responder expects to receive

Docket No. AUS920010449US1

these specifications in a DTD file which follows the standard format, as depicted in **Figure 7**. The initiator receives the responder's selection (step **625**). A Diffie-Hellman key exchange is performed between the
5 initiator and responder (steps **640** and **645**) and authentication data is exchanged depending upon the selected authentication method.

Each party, the initiator and the responder, establishes an Internet Security Association and Key
10 Management Protocol (ISAKMP) Security Association (steps **650** and **655**) to use in securing information sent between the computer systems. In Phase 2 processing, each system creates IPsec Security Associations for securing data traffic sent between the systems by negotiating one or
15 more Security Associations and the systems exchange IP addresses by using phased IDs and policies (steps **660** and **670**, for further details about IDs and policies see **Figure 7**). After the IDs have been exchanged and a security association has been negotiated, each system
20 sends and receives protected data traffic using the established policies and profiles (steps **670** and **675**).

Figure 7 depicts a high level flow chart which illustrates establishing a standard format to use by any operating system and any machine type to automatically
25 configure IP security tunnels in accordance with the present invention. The process starts as depicted by block **700** and thereafter passes to block **702** which illustrates establishing a standard format as a document type definition (DTD) file for specifying IP security
30 tunnels. A DTD file defines a collection of elements that may appear in an XML file. Next, block **704** depicts including a root element in the standard. The following

Docket No. AUS920010449US1

is an example of a root element:

```
<!ELEMENT AIX_VPN ((IKEProtection|IKEGroup|IKETunnel|
    IKEPre-sharedKey|IPSecProposal|
    IPSecProtection|IPSecTunnel)+)>
```

- 5 Any combination of IKEProtection, IKEGroup, IKEPre-sharedKey, IKETunnel, IPSecProposal, IPSecProtection, IPSecTunnel elements may be included in the root element. Any number of occurrences of each element may be included in the root element.
- 10 Block **706** illustrates including a protection element in the standard which includes a listing of IKE transforms. The following is an example of a protection element:

```
<!ELEMENT IKEProtection (IKETransform+)>
15 <!ATTLIST IKEProtection
    IKE_ProtectionName ID #REQUIRED
    IKE_Role (Initiator|Responder|Both|Neither) "Both"
    IKE_XCHGMode (Main|Aggressive) "Main"
    IKE_KeyOverlap CDATA "5"
    IKE_Flags_UseCRL (Yes|No) "No"
20 IKE_ResponderKeyRefreshMaxMinutes CDATA "480"
    IKE_ResponderKeyRefreshMinMinutes CDATA "15"
    IKE_ResponderKeyRefreshMinKB CDATA #IMPLIED
    IKE_ResponderKeyRefreshMaxKB CDATA #IMPLIED
25 >
```

- Thereafter, block **708** depicts including a transform element in the standard. A list of transform elements will be used for phase 1 security associations negotiations. The following is an example of a transform element:
- 30

```
<!ELEMENT IKETransform EMPTY>
<!ATTLIST IKETransform
```

Docket No. AUS920010449US1

```

    IKE_AuthenticationMethod (Preshared_key |
RSA_signatures)

                                "Preshared_key"
    IKE_Encryption (DES-CBC | 3DES-CBC) "3DES-CBC"
5    IKE_Hash (SHA | MD5) "SHA"
    IKE_DHGroup (1 | 2 ) "2"
    IKE_KeyRefreshMinutes CDATA "480"
>

```

The process then passes to block **710** which
 10 illustrates including a group element in the standard.
 This element can contain multiple identification
 elements. The purpose of this element is to allow the
 same protections and policies to be shared by multiple
 IDs. The following is an example of a group element:

```

15 <!ELEMENT IKEGroup (IKEID+)>
    <!ATTLIST IKEGroup
        IKE_GroupName ID #REQUIRED
    >

```

Next, block **712** depicts including an identification
 20 element in the standard. This element includes
 identification types that can be used by both phase 1 and
 phase 2 tunnels. However, not all of the identification
 types are valid in both phases. Phase 1 can use ASN1_DN,
 FQDN, User_FQDN, and KEYID. Phase 2 can use IPV4_Subnet,
 25 IPV6_Subnet, IPV4_Address_Range, and IPV6_Address_Range.
 Both phases can use IPV4_Address and IPV6_Address. The
 protocol and port attributes are only valid in phase 2.
 The following is an example of an identification element:

```

30 <!ELEMENT IKEID (ASN1_DN | FQDN | User_FQDN |
    IPV4_Address |
        IPV6_Address | KEYID | IPV4_Subnet |

```

Docket No. AUS920010449US1

```

IPV6_Subnet |
                IPV6_Address_Range |
IPV4_Address_Range)>
<!ATTLIST IKEID
5         Protocol CDATA "0"
          Port      CDATA "0"
>

```

Thereafter, block **714** illustrates including a tunnel element in the standard. This element defines the phase 1 security association endpoints and the IKEProtection element to be used for the negotiation. The following is an example of a tunnel element:

```

10 <!ELEMENT IKE Tunnel (IKELocalIdentity,
    IKERemoteIdentity)>
15 <!ATTLIST IKE Tunnel
    IKE_TunnelName ID #REQUIRED
    IKE_ProtectionRef IDREF #REQUIRED
    IKE_Flags_MakeRuleWithOptionalIP (Yes | No) "No"
    IKE_Flags_AutoStart (Yes | No) "No"
20 >

```

The "MakeRuleWithOptionalIP" field specifies whether another entry will be put in the rules list using the optional IP address specified in the remote identity element. If this field is set to "no", more than one tunnel can be defined using the same optional IP address; however, the computer system cannot act as a responder in a main mode negotiation with this tunnel. If an optional IP address is specified for the local identity element when the "MakeRuleWithOptionalIP" is set to "no", the optional IP address will be silently discarded as extraneous information for that negotiation type.

Docket No. AUS920010449US1

The process then passes to block **716** which depicts including a local identity element and a remote identity element in the standard. These elements define the local and remote IDs. The following are examples of a local identity element and a remote identity element:

```

5  <!ELEMENT IKELocalIdentity (ASN1_DN | FQDN | User_FQDN |
    IPV4_Address |
    IPV6_Address | KEYID)>
    <!ELEMENT IKERemoteIdentity (ASN1_DN | FQDN | User_FQDN |
10  IPV4_Address | IPV6_Address
    | KEYID |
    IKEGroupRef)>

```

Next, block **718** illustrates including an ID type element in the standard. These following are examples of possible ID type elements which may be included in the standard:

```

15  <!ELEMENT IPV4_Address EMPTY>
    <!ATTLIST IPV4_Address
        Value CDATA #REQUIRED
20  >
    <!ELEMENT IPV4_Subnet EMPTY>
    <!ATTLIST IPV4_Subnet
        IPAddr CDATA #REQUIRED
        Netmask CDATA #REQUIRED
25  >
    <!ELEMENT IPV4_Address_Range EMPTY>
    <!ATTLIST IPV4_Address_Range
        From_IPAddr CDATA #REQUIRED
        To_IPAddr CDATA #REQUIRED
30  >
    <!ELEMENT IPV6_Address EMPTY>
    <!ATTLIST IPV6_Address

```

Docket No. AUS920010449US1

```

Value CDATA #REQUIRED
>
<!ELEMENT IPV6_Subnet EMPTY>
<!ATTLIST IPV6_Subnet
5      IPV6_Addr CDATA #REQUIRED
      IPV6_PrefixLength CDATA #REQUIRED
>
<!ELEMENT IPV6_Address_Range EMPTY>
<!ATTLIST IPV6_Address_Range
10     From_IPV6_Addr CDATA #REQUIRED
      To_IPV6_Addr   CDATA #REQUIRED
>
<!ELEMENT FQDN (IPV4_Address | IPV6_Address)?>
<!ATTLIST FQDN
15     Value CDATA #REQUIRED
>
<!ELEMENT User_FQDN (IPV4_Address | IPV6_Address)?>
<!ATTLIST User_FQDN
      Value CDATA #REQUIRED
20 >
<!ELEMENT ASN1_DN (IPV4_Address | IPV6_Address)?>
<!ATTLIST ASN1_DN
      Value CDATA #REQUIRED
>
25 <!ELEMENT KEYID (IPV4_Address | IPV6_Address)?>
<!ATTLIST KEYID
      Value CDATA #REQUIRED
>

```

30 The process then passes to block **720**, which depicts including a remote pre-shared key ID element in the standard. This element is the ID definition for remote pre-shared key. The following is an example of a remote

Docket No. AUS920010449US1

pre-shared key ID element:

```
<!ELEMENT IKEPresharedRemoteID (PK_ASN1_DN | PK_FQDN |
                                PK_User_FQDN |
                                PK_IPV4_Address |
5                                PK_IPV6_Address |
                                PK_KEYID)>
```

Block **722**, then, illustrates including a pre-shared key element in the standard. This element is the ID definition for the pre-shared key. The following is an example of a pre-shared key element:

```
<!ELEMENT PK_IPV4_Address EMPTY>
<!ATTLIST PK_IPV4_Address
          Value CDATA #REQUIRED
>
15 <!ELEMENT PK_IPV6_Address EMPTY>
    <!ATTLIST PK_IPV6_Address
          Value CDATA #REQUIRED
    >
    <!ELEMENT PK_FQDN EMPTY>
20 <!ATTLIST PK_FQDN
          Value CDATA #REQUIRED
    >
    <!ELEMENT PK_User_FQDN EMPTY>
    <!ATTLIST PK_User_FQDN
25          Value CDATA #REQUIRED
    >
    <!ELEMENT PK_ASN1_DN EMPTY>
    <!ATTLIST PK_ASN1_DN
30          Value CDATA #REQUIRED
    >
    <!ELEMENT PK_KEYID EMPTY>
    <!ATTLIST PK_KEYID
```

Docket No. AUS920010449US1

Value CDATA #REQUIRED

>

Next, block **724** depicts including an IPsec proposal element in the standard. This element includes a list of IPsec encapsulating security protocol (ESP) protocols and/or IPsec authentication header (AH) protocols elements. The following is an example of an IPsec proposal element:

```

5  <!ELEMENT IPsecProposal ((IPsecESPProtocol |
10 IPsecAHProtocol)+)>

```

```

<!ATTLIST IPsecProposal

```

```

    IPsec_ProposalName ID #REQUIRED

```

>

The process then passes to block **726** which illustrates including an IPsec ESP protocol element in the standard. This element defines an IPsec ESP protocol. The following is an example of an IPsec ESP protocol element:

```

<!ELEMENT IPsecESPProtocol EMPTY>

```

```

20 <!ATTLIST IPsecESPProtocol

```

```

    ESP_Encryption (ESP_DES | ESP_3DES | ESP_NULL )
    "ESP_DES"

```

```

    ESP_Authentication (HMAC-MD5 | HMAC-SHA | NONE )
    "HMAC-SHA"

```

```

25    ESP_EncapsulationMode (Tunnel | Transport )
    "Tunnel"

```

```

    ESP_KeyRefreshMinutes CDATA "60"

```

```

    ESP_KeyRefreshKB      CDATA #IMPLIED

```

>

30 Thereafter, block **728** depicts including an IPsec authentication header protocol element in the standard. This element defines an authentication header protocol.

Docket No. AUS920010449US1

The following is an example of an authentication header protocol element:

```

5      <!ELEMENT IPsecAHProtocol EMPTY>
      <!--ATTLIST IPsecAHProtocol
          AH_Authentication (AH_MD5 | AH_SHA ) "AH_SHA"
          AH_EncapsulationMode (Tunnel | Transport )
            "Tunnel"
          AH_KeyRefreshMinutes CDATA "60"
          AH_KeyRefreshKB      CDATA #IMPLIED
10  >

```

Next, block **730** illustrates including an IPsec protection element in the standard. This element defines IPsec protection. The following is an example of an IPsec protection element:

```

15  <!ELEMENT IPsecProtection EMPTY>
      <!--ATTLIST IPsecProtection
          IPsec_ProtectionName ID #REQUIRED
          IPsec_ProposalRefs IDREFS #REQUIRED
          IPsec_Role (Initiator|Responder|Both|Neither)
20  "Both"
          IPsec_KeyOverlap      CDATA "5"
          IPsec_Flags_UseCommitBit (Yes | No) "No"
          IPsec_Flags_UseLifeSize (Yes | No) "No"
          IPsec_InitiatorDHGroup (0 | 1 | 2 ) "0"
25  IPsec_ResponderDHGroup (NO_PFS | GROUP_1 |
            GROUP_2 |
                                GROUP_1_OR_2 |
                                NO_PFS_OR_GROUP_1_OR_2)
                                "NO_PFS_OR_GROUP_1_OR_2"
30  IPsec_ResponderKeyRefreshMaxMinutes CDATA "120"
          IPsec_ResponderKeyRefreshMinMinutes CDATA "1"
          IPsec_ResponderKeyRefreshMaxKB CDATA #IMPLIED

```

Docket No. AUS920010449US1

IPSec_ResponderKeyRefreshMinKB CDATA #IMPLIED

>

The process then terminates as depicted by block **732**.

Figure 8 illustrates a high level flow chart which depicts automatically configuring an IP security tunnel using a standard format in accordance with the present invention. The process starts as depicted by block **800** and thereafter passes to block **802** which depicts generating an XML file under the guidelines of the standard format defined by the DTD file described in more detail in **Figure 7**. Next, block **804** illustrates including elements from the standard as necessary to properly configure an IP security tunnel. Thereafter, block **806** depicts processing the XML file. Processing this file automatically configures an IP security tunnel. The process then terminates as depicted by block **808**.

Below is an example of an XML file that configures a tunnel under the guidelines of the standard.

```
<?xml version="1.0" ?>
20 <!DOCTYPE AIX_VPN SYSTEM "ike.dtd">

<AIX_VPN>

<!-- Define a Phase 1 policy -->
25 <IKEProtection IKEProtectionName="IBM_low_CertSig"
      IKEResponderKeyRefreshMinTime="300"
      IKEResponderKeyRefreshMaxTime="81400">

      <!-- Define the transforms underneath this
30 IKEprotection -->
      <IKETransform AuthMethod="RSASignature" Encrypt="DES"
        Hash="SHA" IKEDHGroup="1"/>
```

```
<IKETransform AuthMethod="PresharedKey"
IKEDHGroup="1"/>
</IKEProtection>
```

```
<IKEGroup IKEGroupName="P1Group_shruthi">
```

```
10      </ASN1_DN>
```

<IPV4_Address Value="9.53.150.11"/>

<IPV4 Address Value="9.53.150.11"/>

```
<IKE Tunnel IKE TunnelName="P1_Apricot"
```

<IPV4 Address Value="9.3.97.138"/>

<IPV4_Address Value="9.3.97.66"/>

```
<!-- Define the phase 1 Tunnel with remote-id being a
group name -->
```

<IKELocalIdentity>

Docket No. AUS920010449US1

```
<IPV4_Address Value="9.3.97.138"/>
</IKELocalIdentity>
<IKERemoteIdentity>
  <IKEGroupRef IKEGroupNameRef="P1Group_shruthi"/>
5  </IKERemoteIdentity>
</IKETunnel>

<!-- Specify the preshared keys for the 9.3.97.138 &
9.53.150.11 -->
10 <IKEPresharedKey Value='abcd>'>
  <IKEPresharedRemoteID>
    <IPV4_Address Value="9.53.150.11"/>
  </IKEPresharedRemoteID>
</IKEPresharedKey>
15

<!-- Define a Phase 2 proposal -->
<IPSecProposal ProposalName="IBM_ESP_tunnel_Proposal">
  <IPSecProtocol Protocol="ESP" ESP_Encryption="DES"
20     ESP_Authentication="HMAC-MD5"
    KeyRefreshTime="28800"/>
</IPSecProposal>

<IPSecProtection
25 IPSecProtectionName="IBM_ESP_tunnel_policy"
    IPSecInitiatorDHGroup="1"
    IPSecKeyRefreshMinTime="120"
    IPSecKeyRefreshMaxTime="81400"

30 IPSecProposalRefs="IBM_ESP_tunnel_Proposal"/>

<IPSecTunnel IPSecTunnelName="P2_Apricot"
```

Docket No. AUS920010449US1

IKETunnelName="Pl_Apricot"

IPSecProtectionRef="IBM_ESP_tunnel_policy">

<IPSecLocalIdentity>

<IPV4_Address Value="9.3.97.138"/>

5 </IPSecLocalIdentity>

<IPSecRemoteIdentity>

<IPV4_Address Value="9.3.97.66"/>

</IPSecRemoteIdentity>

</IPSecTunnel>

10

</AIX_VPN>

15 In this example, explicit policy and tunnel choices are being specified, namely using RSA signature mode for authentication with Diffie Helmann group 1 with local identity 9.3.97.138 and remote identity 9.3.97.66. In this example, the use of DES with HMAC-MD5 and a refresh time of 28800 seconds are requested.

20 It is important to note that while the present invention has been described in the context of a fully functioning data processing system, those of ordinary skill in the art will appreciate that the processes of the present invention are capable of being distributed in the form of a computer readable medium of instructions and a variety of forms and that the present invention
25 applies equally regardless of the particular type of signal bearing media actually used to carry out the distribution. Examples of computer readable media include recordable-type media, such as a floppy disk, a hard disk drive, a RAM, CD-ROMs, DVD-ROMs, and
30 transmission-type media, such as digital and analog communications links, wired or wireless communications links using transmission forms, such as, for example,

Docket No. AUS920010449US1

radio frequency and light wave transmissions. The computer readable media may take the form of coded formats that are decoded for actual use in a particular data processing system.

5 The description of the present invention has been presented for purposes of illustration and description, and is not intended to be exhaustive or limited to the invention in the form disclosed. Many modifications and variations will be apparent to those of ordinary skill in
10 the art. The embodiment was chosen and described in order to best explain the principles of the invention, the practical application, and to enable others of ordinary skill in the art to understand the invention for various embodiments with various modifications as are
15 suited to the particular use contemplated.